CLAIMS

What is claimed is:

1. An apparatus comprising:

a quotient pre-calculation array (QPA);

a main array ; and

a quotient pre-calculation circuit, to ensure a true remainder during a following cycle is evenly divisible by a radix.

2. The apparatus of claim 1 wherein the main array and the QPA comprises:

a first multiplicand-add multiplexer (MAM) in the main array to couple at least a multiplicand bit with a first carry save adder (CSA) in the main array;

a first modulus-add multiplexer (MM) in the QPA to couple at least a modulus bit with a first CSA in the QPA;

a second CSA in the main array coupled with the first CSA in the main array and with a first MM in the main array; and

a second CSA in the QPA coupled with the first CSA in the QPA, and with a second MM in the QPA.

3. The apparatus of claim 2, wherein the quotient pre-calculation circuit is coupled with the second MM in the QPA, the second MM in the main array, and with the first MM in the QPA.

4. An apparatus as in claim 1, wherein the main array is optimized for area, and the quotient pre-calculation array is optimized for speed.

5. An apparatus as in claim 2 wherein the CSAs have three inputs, a sum output and a carry output.

6. An apparatus as in claim 2 wherein the second CSA in the main array is further coupled to the first CSA in the QPA through a flip-flop.

7. An apparatus as in claim 2, wherein the second CSA in the QPA is coupled to a buffer.

8. An apparatus as in claim 2, wherein the MAM is coupled to at least one multiplier bit.

9. An apparatus as in claim 2 wherein, the second MM in the main array and the first MM in the QPA are coupled to the quotient pre-calculation array via a flip-flop.

10. An apparatus as in claim 2, wherein the QPA processes Q bits of a Montgomery multiplication, and the main array processes N-Q bits of the Montgomery multiplication.

11. An apparatus as in claim 10 wherein the main array is Q bits to the left of the quotient pre-calculation array.

12. An apparatus comprising:

a quotient pre-calculation array (QPA), an add-one array, and a main array comprising

a first multiplicand-add multiplexer (MAM) in the main array to couple at least a multiplicand bit with a first carry save adder (CSA) in the main array;

a first modulus-add multiplexer (MM) in the QPA to couple at least a modulus bit with a first CSA in the QPA;

a first add-one multiplexer (AOM) in the add-one array to couple at least a binary one bit with a first CSA in the add-one array;

a second CSA in the main array coupled with the first CSA in the main array and with a first MM in the main array;

a second CSA in the QPA coupled with the first CSA in the QPA, and with a second MM in the QPA;

a second CSA in the add-one array coupled with the first CSA in the add-one array, and with a first MM in the add-one array; and

a quotient pre-calculation circuit, to pre-calculate a quotient, coupled with the second MM in the QPA, the second MM in the main array, and with the first MM in the QPA.

13. An apparatus as in claim 12, wherein the first add-one multiplexer is coupled to at least one multiplier bit via flip-flops.

14. An apparatus as in claim 12, wherein the second CSA in the main array is further coupled to the first CSA in the add-one array, and the second CSA in the add-one array is coupled to the first CSA in the QPA through one or more flip-flops.

15. A method comprising:

adding at least one multiplicand bit from a first multiplicand-add multiplexer in a main array of a Montgomery multiplier with at least one modulus bit from a first modulus-add multiplexer in the main array;

adding at least one modulus bit from a first modulus-add multiplexer in a quotient pre-calculation array with at least one modulus bit from a second modulus-add multiplexer in the quotient pre-calculation array;

pre-calculating the quotient during a first cycle; and

sending at least one value to control the first modulus-add multiplexer in the main array, the first modulus-add multiplexer in the quotient pre-calculation array, and the second modulus-add multiplexer in the quotient pre-calculation array so that the value of the quotient is evenly divisible by the radix during a second cycle through the Montgomery multiplier.

16. A method as in claim 15, further comprising performing an additional cycle through the Montgomery multiplier to synchronize the bits in the main array and in the quotient pre-calculation array.

17. A method as in claim 15, wherein during the additional cycle the second modulus-add multiplexer outputs a 0 bit.

18. A method as in claim 15 further comprising inserting a 1 bit when necessary to complete a 2's complement of the multiplicand.

19. A method as in claim 15 wherein the first multiplicand-add multiplexer has values at its inputs consisting at least one of -2 x the multiplicand , -1 x the multiplicand, 0, 1 x the multiplicand, and 2 x the multiplicand.

20. An apparatus comprising:

means for adding at least one multiplicand bit from a first multiplicand add multiplexer in a main array of a Montgomery multiplier with at least one modulus bit from a first modulus-add multiplexer in the main array;

means for adding at least one modulus bit from a first modulus-add multiplexer in a quotient pre-calculation array with at least one modulus bit from a second modulus-add multiplexer in the quotient pre-calculation array;

means for pre-calculating the quotient during a first cycle; and

means for sending at least one value to control the first modulus-add multiplexer in the main array, the first modulus-add multiplexer in the quotient pre-calculation array, and the second modulus-add multiplexer in the quotient pre-calculation array so that the value of the quotient is evenly divisible by the radix during a second cycle through the Montgomery multiplier.

21. An apparatus as in claim 20, further comprising means for performing an additional cycle through the Montgomery multiplier to synchronize the bits in the main array and in the quotient pre-calculation array.

22. An apparatus as in claim 20, wherein the means for pre-calculating the quotient causes the second modulus-add multiplexer to output a 0 bit during the additional cycle through the Montgomery multiplier.